AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Andrew R. Ubbelohde, Special Agent, Federal Bureau of Investigation (FBI), United States Department of Justice, being duly sworn, state:

I. INTRODUCTION

1. I am a Special Agent with the FBI. As such, I am "an investigative or law enforcement officer of the United States," within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States empowered by law to conduct investigations and make arrests for offenses enumerated in 18 U.S.C. § 2516. I entered the FBI in June of 2016. I have been a Special Agent in Billings, Montana since November of 2016. I spent approximately six months investigating violent crimes on Indian Reservations and subsequently have been assigned to the Big Sky West Transnational Organized Crime Task Force. The main focus of this task force is to investigate, disrupt, and dismantle illegal drug trafficking organizations.

2. Throughout my career, I have received specialized training relating to several law enforcement topics.

3. Specifically, I have conducted or assisted with investigations relative to the manufacture, smuggling and distribution of controlled substances and the subsequent illicit transfer and laundering of the proceeds derived from the sale of controlled substances. I have also participated in numerous narcotics investigations which have resulted in the seizure of large quantities of controlled

substances, firearms, cash currency, and contraband associated with violations of Title 18 and Title 21 of the United States Code. I am familiar with, and have participated in, all of the normal methods of investigation, including but not limited to visual surveillance, questioning of witnesses, the use of search and arrest warrants, the use of informants, the use of pen registers, the utilization of undercover agents, the use of Grand Jury, and the use of court authorized wire and electronic intercepts. Additionally, I have consulted with other Agents who have been involved in similar and unrelated investigations.

4. Throughout my career, I have discussed with numerous law enforcement officers, cooperating defendants, and informants, the methods and practices used by gang members and narcotics distributors and I am familiar with their typical methods of operation, including, the manufacturing, distribution, storage and transportation of narcotics, and the collection of money which represents the proceeds of narcotics trafficking and money laundering.

II. BACKGROUND ON THE DARK WEB AND CRYPTOCURRENCY

5. I am familiar with the following relevant terms and definitions:

6. The "dark web" is a portion of the "Deep Web[1]" of the Internet, where individuals must use an anonymizing software or application called a

[1] The Deep Web is the portion of the Internet not indexed by search engines. Examples are databases and internal networks belonging to private industry, government agencies, or academic institutions.

"darknet" to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply the "web"). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring. Famous dark web marketplaces, also called Hidden Services, such as Silk Road, AlphaBay, and Hansa (all of which have since been shut down by law enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services.

7. "Vendors" are the dark web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts" on dark web marketplaces. Customers, meanwhile, operate "customer accounts." Vendor and customer accounts are not identified by numbers, but rather monikers or "handles," much like the username one would use on a clear web site. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces, and based on seller and customer reviews, can become well known as "trusted" vendors or customers. It is also possible for the same person to operate

multiple customer accounts and multiple vendor accounts at the same time. For example, based on my training and experience, I know that one person could have a vendor account that he or she uses to sell illegal goods on a dark web marketplace in exchange for cryptocurrency; that same vendor could also have a different customer account that he or she uses to exchange cryptocurrency earned from vendor sales for fiat currency.2 Because they are separate accounts, a person could use different accounts to send and receive the same cryptocurrency on the dark web. I know from training and experience that one of the reasons dark web vendors have multiple monikers for different vendor and customer accounts, is to prevent law enforcement from identifying which accounts belong to the same person, and who the actual person is that owns or uses the accounts.

8. The "Tor network," or simply "Tor" (an abbreviation for "The Onion Router"), is a special network of computers on the Internet, distributed around the world, designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such hidden services operating on Tor have complex web addresses, generated by a computer algorithm,

2 Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

ending in ".onion" and can only be accessed through specific web browser software, including a browser known as "Tor Browser," designed to access the Tor network. Examples of hidden services websites are the aforementioned AlphaBay and Hansa. Tor is available on cellphones using the Android and Apple operating systems by installing an application that puts a TOR-enabled internet browser on a user's cellphone, which then routes the phone's IP address through different servers all over the world, making it extremely difficult to track.

9. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a

distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.3 Cryptocurrency is not illegal in the United States.

10. Bitcoin4 ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public

3 Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

4 Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it's not completely anonymous, bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

11. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26–25 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

12. Although cryptocurrencies such as bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering, and is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces. As of January 8th, 2019, one bitcoin is worth approximately $4,000.06 though the value of bitcoin is generally much more volatile than that of fiat currencies.

13. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb

drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code5 with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

14. Bitcoin "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses. Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered

5 A QR code is a matrix barcode that is a machine-readable optical label.

money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers that the customer links to an exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who lack AML or KYC protocols and often also advertise their ability to offer customers stealth and anonymity. These illicit exchangers routinely exchange fiat currency for cryptocurrencies by meeting customers in person or by shipping cash through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9–10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1–2%).

15. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not

store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet.

III. PURPOSE OF AFFIDAVIT

16. This Affidavit is submitted in support of an application for a search and seizure warrant of the items listed in Attachment A, which are twenty-two accounts and account authentication credentials, as well as yet to be identified similar accounts. This Affidavit requests the authority to access and search the accounts using the account authentication credentials (username, password, PINS, PGP encryption phrases, etc.). For almost all of these accounts I have been

advised by a cyber-trained agent that the service provider either a) does not maintain logs or records, b) is not cooperative with legal process, and/or c) is located in a jurisdiction that is beyond the legal jurisdiction of the United States. For most of the accounts the only way to effectively search the online account for evidence of a crime would be to directly access the accounts using the authentication credentials which were discovered during the course of this investigation. The items to be seized from the virtual accounts are specifically described in Attachment B, which constitute the fruits, instrumentalities, and evidence of violations 21 U.S.C § 841 (a) (1) and 846.:

17. These accounts are described further in Attachment A and will be referred to as "ACCOUNTS" hereafter. The statements in this Affidavit pertain to the investigation described below and are based in part on information provided by my own observations and experience as an FBI Agent, and the observation and experiences of other fellow law enforcement officers participating in the investigation. This Affidavit does not purport to contain all facts related to this investigation, but only those facts necessary to establish probable cause with respect to the aforementioned offense.

18. I further submit that there is probable cause to believe that Green's cryptocurrency (hereafter, SUBJECT'S ASSETS) constitute (1) moneys, negotiable instruments, securities, or other things of value furnished or intended to

be furnished in exchange for a controlled substance, in violation of the Controlled Substances Act ("CSA"); (2) proceeds traceable to such an exchange; or (3) moneys, negotiable instruments, or securities used or intended to be used to facilitate a violation of the CSA. Subject's assets are therefore subject to forfeiture to the United States under 21 U.S.C. § 881(a)(6).

19. I additionally submit there is probable cause to believe that the SUBJECT'S ASSETS constitute property involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or are traceable to such property. SUBJECT'S ASSETS are, therefore, subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1) (civil forfeiture) and 982(a)(1) (criminal forfeiture).

IV. BACKGROUND OF THE INVESTIGATION

20. On December 18th, 2018, at approximately 0300 hours an Ontario plated truck arrived at the Blue Water Bridge in Port Huron, MI. The truck was a Canadian Cartage carrying the commodity of Canadian mail destined for the United States. The truck was referred to the Blue Water Bridge Centralized Examination Station (CES) for an intrusive exam for narcotics interdiction/enforcement. Customs and Border Patrol Officers (CBPO) were assigned to complete the examination at the CES. During the examination the CBPO's opened a package from, "Roy Paul, 203 Pine St., Kingston, Ontario

Canada K7K1W6" addressed to "Gregory Green 1716 Westwood Dr., Billings, MT 59102". The package was labeled "Organic Fitness Vitamin" with a tracking #LM108118. Upon CBPO opening the package they found a vacuum sealed package containing green pills marked S/90/3. These pills were found to be Xanax pills. Xanax pills are classified as schedule IV and thus require a doctor's prescription to be legally obtained. The package was turned over to Homeland Security Investigator (HSI) Special Agent Leonard. The pills were counted and totaled 1,471 pills. The pills were placed in a seizure bag along with the original packaging. HSI Special Agent Leonard contacted HSI Special Agent Barrera who works in Billings at the Eastern Montana High Intensity Drug Trafficking Area Task Force (EM-HIDTA TF) and forwarded the package to him.

21. Agents contacted the US Postal Inspector for Montana, Walt Tubbs. He stated he would assist Agents in a controlled delivery if needed. He also provided Agents with a list of packages to the residence of 1716 Westwood Dr. since 12/20/17. The list contained approximately 112 packages from various locations to include 13 packages originating in Canada.

22. Agents researched Gregory Green and did not find him locally listed. Using a nationwide people search (TLO), Agents found a Gregory P. Green with a Date of Birth of XX-XX-1955 listed at 1716 Westwood Dr. A criminal history check on Gregory Green showed arrests for arson, theft and disorderly conduct

from 1975 to 1981. Brittany Green, Gregory Green's daughter, also resides at 1716 Westwood Dr. Criminal history checks revealed multiple felony drug charges against her.

23. On January 2nd, 2019, Agents with the EMHIDTA wrote an anticipatory District Court of Montana search warrant for the address of 1716 Westwood Dr. The search warrant execution was contingent on the package being delivered and taken into the residence. The search warrant was presented to District Court of Montana Judge Harris of the Thirteenth Judicial District, Yellowstone County. After reviewing the warrant, Judge Harris signed it.

24. In the early morning of January 3rd, 2019, Agents began surveillance on the residence. At approximately 0938 hours United States Postal Inspector Tubbs delivered the package to the residence. An older female answered the door, took possession of the package and took it inside. After a few minutes, Agents approached the residence and executed the search warrant.

25. In addition to an elderly female (Jeannine Roberts), Agents located Gregory Green in an upstairs office and Brittany Green in a downstairs bedroom. All the occupants were taken outside to be identified and interviewed. When Agents were in the basement they located a living room and an adjacent bedroom that was littered with drugs and drug paraphernalia to include what Agents

believed to be a clandestine methamphetamine lab which included a pan and heat source, various chemicals, and white powdery substance.

26. The Billings Fire Department Hazmat team was called to the scene to assist Agents in determining what was located in the basement and if it was a safety concern.

27. Brittany Green was taken to a vehicle and identified. For officer safety and public safety reasons Agents began to ask questions about what was located downstairs. She told Agents that she was a drug addict and she "washed" methamphetamine. She was under the influence of narcotics and could not fully explain what was downstairs and what it was used for. After being advised of her Miranda Rights she requested a lawyer.

28. Detective Buechler and FBI TFO Detective Robinson attempted to interview Gregory Green but he did not wish to provide information.

29. Detective Buechler and Detective Robinson interviewed Jeannine Roberts, Date of Birth XX-XX-1933. She provided background information on herself and Gregory Green. She described themselves as anti-social people that seldom leave the residence and have no family or friends. She explained how Gregory had an office that he works out of and that his daughter, Brittany, lives in the basement. Jeannine Roberts stated that neither Gregory nor Brittany had a job. She stated she had no information on drug activity or the comings and goings of

packages from the residence. After speaking to her she left the area and returned after Agents were done.

30. As Agents conducted interviews, the Billings Fire Department entered the residence and determined the house not to be a public safety risk and Agents could complete the search warrant with proper personnel protection equipment.

31. As Agents began to search the residence it was evident that this was a very large scale drug operation being run from the residence. One of the computers in Gregory Green's room displayed the "dark web" and showed a screen where he was selling Xanax bars to people across the county using bitcoin as currency. There was physical documentation in the office that showed he was using cryptocurrency wallets. These included pins, passwords, and recovery pins. Furthermore, a review of files located on the desktop of the computer in the office revealed multiple cryptocurrency wallet files.

32. Throughout his office, bedroom and also Brittany Green's bedroom and living room area Agents located hundreds of items of drug paraphernalia. One item in his office was a sealed (ready to be sent) package. In the package was a plastic wrapped metal container made to look like a bandage container with a homemade label. Inside this container was a sealed baggie containing approximately 7 grams of suspected methamphetamine and two Xanax bars. There was packaging material in the residence to send hundreds of items through the mail

similar to this. In the Office Agents seized approximately 100 grams of suspected methamphetamine, several thousand Xanax bars as well as other scheduled drugs and other items of evidence. In the basement Agents seized approximately 122 grams of suspected methamphetamine, ketamine, carfentanil and other controlled drugs. Also located in the basement were hundreds of feet of glass tubing that were being made into glass pipes, a 100 pound butane tank and instructions/ recipes for Brittany Green on how to combine drugs for distribution. A sample of the suspected methamphetamine was tested using a NIK kit and it tested positive for methamphetamine.

33. Agents arrested Gregory Green and Brittany Green and transported them to the Yellowstone County Detention Center.

34. Pursuant to the signed warrant, Agents seized and analyzed computers located in Gregory Green's office. As a result of that analysis, Agents believe Gregory Green is storing his drug distribution proceeds in cryptocurrency.

35. Furthermore, Agents applied for and were granted a subsequent federal search warrant for 1716 Westwood Dr as well as for unopened packages addressed to Greg Green seized in the initial search warrant. This second search revealed numerous additional physical pages which appeared to contain passwords, key phrases, etc. which appeared to pertain to online/darkweb accounts as well as

other documentation relating to drug trafficking. Also, three of the packages contained approximately 1,500 Xanax pills each.

V. Conclusion

35. Based upon my knowledge of the overall investigation, I believe Gregory Green has been operating a sophisticated drug distribution operation from his residence in Billings, MT and a key component of the operation is his use of darkweb applications. Through my knowledge of the proceeds generated by the distribution of illegal drugs, from information told to me by cyber trained Agents, and finally by the initial assessment of the configuration of Gregory Green's distribution operation, I believe it is highly probable that illegal drug proceeds are being kept in Gregory Green's virtual accounts. This belief is underscored by Agents seeing evidence of drug transactions on Gregory Green's computer which used bitcoin as currency as well as evidence that Green has evidence of a bitcoin account/wallet on the same machine. Furthermore, from consultations with specifically trained cyber agents with years of experience these accounts are indicative of online darkweb merchant accounts and anonymous email communication accounts.

///

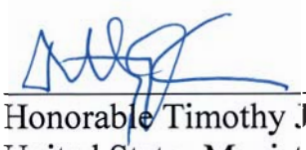
///

///

36. I swear that the facts presented herein are true and accurate to the best of my knowledge.

Andrew R. Ubbelohde
Special Agent
Federal Bureau of Investigation

SWORN AND SUBSCRIBED TO BEFORE ME THIS 11th DAY OF JANUARY, 2019.



Honorable Timothy J. Cavan
United States Magistrate Judge
District of Montana